UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/619,176	07/15/2003	Max Hamberg	59643.00215	4987

32294 7590 01/10/2007

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/619,176	HAMBERG ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-54 are presented for examination.

Claim Objections

2. Claims 1, 18-20, 35-37, 40-43 and 49-53 are objected to because of the following informalities:

a) As to claim 1, the phrase "generating a second set of data representative of a first set of data" should be "generating a second set of data representative of the first set of data".

b) As to claim 18, the phrase "steps of decrypting the encrypted first set of data and transmitting a request to download the encrypted first set of data to the address of a location at which the encrypted first set of data is stored" should be "steps of transmitting a request to download the encrypted first set of data to the address of a location at which the encrypted first set of data is stored and decrypting the encrypted first set of data".

c) As to claim 19, the phrase "steps of decrypting the encrypted first set of data and downloading the encrypted set of data from the first node to the second node" should be "steps of downloading the encrypted first set of data from the first node to the second node and decrypting the encrypted first set of data".

d) As to claim 20, the phrase "steps of decrypting the encrypted first set of data and downloading the second set of data from the third node to the second node"

should be "steps of downloading the second set of data from the third node to the second node and decrypting the encrypted first set of data".

e) As to claims 35-36, the phrase "A system according to claim 33" should be "A system as claimed in claim 34".

f) As to claim 37, the phrase "A system as claimed in claims 33" should be "A system as claimed in claim 34".

g) As to claims 40-42, the phrase "A system as claimed in claim 33" should be "A system as claimed in claim 38" (based on antecedent dependency basis of "the second node").

h) As to claims 43 and 49-53, the phrase "A system as claimed in claim 33" should be "A system as claimed in claim 34".

i) As to claim 52, being depend on claim 34 as suggested, the phrase "from the first node" should be "from a first node".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 4-5, 27, 34-35, 43, 49 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317).

a) As to claim 1, Fronberg discloses a method of encrypting a first set of data (e.g. software program, see Fronberg: paragraph 0048) comprising the steps of generating a second set of data (e.g. checksum) representative of the first set of data (i.e. checksum information is associated with the software program, see Fronberg: paragraph 0048); and encrypting the first set of data using the second set of data (i.e. encrypting the software program using the encryption/decryption key deriving from the checksum, see Fronberg: paragraph 0048). Fronberg discloses using checksum to derive a unique encryption/decryption key, however he does not explicitly disclose checksum (i.e. second set of data) is a representative of a first set of data. Checksum is known in the art as a mechanism of protecting data integrity, checksum is computed by adding up the basic components of a message, typically the asserted bits, and storing the resulting value (i.e. representative of a message, itself). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ checksum as a generated representative of the first set of data in the system of Fronberg so as to make encryption/decryption key more unique by deriving the key from a checksum (see Fronberg: paragraph 0048).

b) As to claim 2, Fronberg discloses a method as claimed in claim 1, wherein the first set of data is encrypted by performing a symmetric key based encryption algorithm (i.e. the same key is used for encryption and decryption) between the first set of data and the second set of data (see Fronberg: paragraph 0047).

c) As to claim 4, Fronberg discloses a method as claimed in claim 1, wherein the first set of data comprises digital data (i.e. software program, see Fronberg: paragraph 0030).

d) As to claim 5, Fronberg discloses a method as claimed in claim 1, wherein the second set of data comprises a reduced version of the first set of data (i.e. checksum is the reduced version, see Fronberg: paragraph 0048).

e) As to claim 27, Fronberg discloses a method as claimed in claim 1, wherein the first set of data comprises one of a digital photograph, a picture or a text document, an audio file or multimedia message (i.e. software program, see Fronberg: paragraph 0030).

f) As to claim 34, this claim is directed to a system implementation of the method of claim 1, therefore it is rejected by a similar rationale applied against claim 1 above.

g) As to claim 35, this claim is directed to a system implementation of the method of claim 2, therefore it is rejected by a similar rationale applied against claim 2 above.

h) As to claim 43, Fronberg discloses a system as claimed in claim 34, further comprising decrypting means for decrypting the encrypted first set of data using the second set of data (i.e. using the second set of data as a symmetric key, therefore the same key is used for both encryption and decryption, see Fronberg: paragraph 0047).

i) As to claim 49, Fronberg discloses a system as claimed in claim 34, wherein the first set of data comprises one of a digital photograph, a picture or a text document, an audio file or multimedia message (i.e. software program, see Fronberg: paragraph 0030).

j) As to claim 51, Fronberg discloses a system as claimed in claim 34, wherein the system comprises a single entity (see Fronberg: Fig. 1, element 112).

5. Claims 3, 36, 38 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Schneier (Applied Cryptography).

a) As to claim 3, Fronberg discloses a method as claimed in claim 1, however he is silent on the capability of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data. Schneier is relied on for the teaching of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data (i.e. the plaintext is being XORed with a keyword to generate the ciphertext, see Schneier: page 14). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data in the system of Fronberg, as Schneier teaches, so as to provide another way of encrypting data.

b) As to claim 36, this claim is directed to a system implementation of the method of claim 3, therefore it is rejected by a similar rationale applied against claim 3 above.

c) As to claim 38, the combination of Fronberg and Schneier discloses a method as claimed in claim 36, further comprising a second node comprising storage means configured to store the second set of data (i.e. storing in a computer, see Fronberg: Fig. 1, element 112; paragraphs 0027, 0050).

d) As to claim 40, the combination of Fronberg and Schneier discloses a method as claimed in claim 38, wherein the second node further comprises the encrypting means (see Fronberg: paragraphs 0046-0048).

6. Claims 6-7, 9-11, 16, 18-19, 21-24, 26, 29-30, 37, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Suzuki et al. (6,704,119).

a) As to claim 6, Fronberg discloses a method as claimed in claim 1, however he is silent on the capability of having an encrypted first set of data is stored at a first node. Suzuki is relied on for the teaching of having an encrypted first set of data (i.e. first set of data is generated by multi-function peripheral (MFP) (see Suzuki: Fig. 1, element 11; col. 4, lines 59-61; col. 5, lines 27-28) is stored at a first node (e.g. server, see Suzuki: col. 6, lines 48-50; col. 12, lines 36-39). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having an

encrypted first set of data is stored at a first node in the system of Fronberg, as Suzuki teaches, so as to store and archive file data (see Suzuki: col. 1, lines 15-22).

b) As to claim 7, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, further comprising the step of storing the second set of data in a memory of a second node (i.e. storing in a computer, see Fronberg: Fig. 1, element 112; paragraphs 0027, 0050).

c) As to claim 9, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, further comprising the steps of transmitting the encrypted first set of data from the second node (e.g. MFP) to the first node (e.g. server, see Suzuki: col. 12, lines 36-39).

d) As to claim 10, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, further comprising the step of storing the encrypted first set of data at a location on said first node (see Suzuki: col. 9, lines 1-5).

e) As to claim 11, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, further comprising the step of transmitting address information of a location at which the first set of data is stored from the first node to said second node (i.e. location specified in additional data is supplied in the transmission instruction indicates location address is provided and now being used to access data in the server, see Suzuki, col. 6, lines 23-30).

f) As to claim 16, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, further comprising the step of decrypting the encrypted first set of data using the second set of data (i.e. using the second set of data as a

symmetric key, therefore the same key is used for both encryption and decryption, see Fronberg: paragraph 0047).

g) As to claim 18, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, further comprising the steps of decrypting the encrypted first set of data (i.e. encrypting/decrypting process using the same key, see Fronberg: paragraphs 0046-0048), and transmitting a request to download the encrypted first set of data to the address of a location at which the encrypted first set of data is stored (i.e. document data is encrypted in the image processing unit of MFP 11, then is transmitted and stored in server 12, see Suzuki: col. 12. lines 36-39; encrypted document data is transmitted to MFP 11, see Suzuki: col. 6, lines 48-50).

h) As to claim 19, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, further comprising the steps of decrypting the encrypted first set of data (i.e. encrypting/decrypting process using the same key, see Fronberg: paragraphs 0046-0048) and downloading the encrypted first set of data from the first node to the second node (encrypted document data is transmitted to MFP 11, see Suzuki: col. 6, lines 48-50).

i) As to claim 21, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, wherein the second set of data is generated at a second node (i.e. checksum is generated in a computer, see Fronberg: paragraph 0048).

j) As to claim 22, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, wherein the first set of data is encrypted at the second

node (i.e. the software program is encrypted in a computer, see Fronberg: paragraph 0048).

k) As to claim 23, the combination of Fronberg and Suzuki discloses a method as claimed in claim 6, wherein the first node comprises a first network archive server (e.g. server 12, see Suzuki: col. 6, lines 31-40, lines 48-57).

l) As to claim 24, the combination of Fronberg and Suzuki discloses a method as claimed in claim 7, wherein the second node comprises a piece of user equipment (i.e. computer, see Fronberg: Fig. 1, element 112).

m) As to claim 26, the combination of Fronberg and Suzuki discloses a method as claimed in claim 24, wherein the user equipment comprises one of a mobile station, a digital camera, a personal digital assistant or a personal computer (i.e. computer, see Fronberg: Fig. 1, element 112).

n) As to claim 29, the combination of Fronberg and Suzuki discloses a method as claimed in claim 7, wherein the first set of data is created by the second node (i.e. software programs, i.e. instructions, are in the computer, see Fronberg: paragraph 0027).

o) As to claim 30, the combination of Fronberg and Suzuki discloses a method as claimed in claim 7, wherein the first set of data is received at the second node from a third party (e.g. PC 14, see Suzuki: col. 6, lines 6-8).

p) As to claim 37, this claim is directed to a system implementation of the method of claim 6, therefore it is rejected by a similar rationale applied against claim 6 above.

q) As to claim 46, the combination of Fronberg and Suzuki discloses a system as claimed in claim 37, wherein the second node comprises a piece of user equipment (i.e. computer, see Fronberg: Fig. 1, element 112).

7. Claims 8, 12-15, 20, 25 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Suzuki et al. (6,704,119) and further in view of Marvit et al. (6,625,734).

a) As to claim 8, the combination of Fronberg and Suzuki discloses a method as claimed in claim 7, however it is silent of the capability of storing the second set of data at a third node. Marvit is relied on for the teaching of storing the second set of data (e.g. unique key associated with message ID) at a third node (e.g. key repository) (i.e. storing key in the key repository, see Marvit: col. 4, lines 41-43). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing the second set of data at a third node in the system of Fronberg and Suzuki, as Marvit teaches, so as to securely and effectively control and track access to data (see Marvit: col. 3, lines 60-61).

b) As to claim 12, the combination of Fronberg and Suzuki discloses a method as claimed in claim 11, however it is silent on the capability of having the address information of the location at which the encrypted first set of data is stored is a URL. Marvit is relied on for the teaching of having the address information of the location at which the encrypted first set of data is stored is a URL (i.e. the recipient is provided with a message's URL that specifies the location of the message, see Marvit:

col. 19, lines 55-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the address information of the location at which the encrypted first set of data is stored is a URL in the system of Fronberg and Suzuki, as Marvit teaches, so as to control and track access to data on communication network (see Marvit: col. 2, lines 1-5).

c) As to claim 13, the combination of Fronberg, Suzuki and Marvit discloses a method as claimed in claim 8, further comprising the step of storing the second set of data at a location on said third node (i.e. storing the second set of data at a specific location on the key repository, see Marvit: Fig. 2, element 204).

d) As to claim 14, the combination of Fronberg, Suzuki and Marvit discloses a method as claimed in claim 13, further comprising the step of transmitting address information of the location at which the second set of data is stored from said third node to said second node (i.e. the combination of Fronberg and Suzuki teaches transmitting address information of a location at which the first set of data is stored from the first node to said second node (i.e. location specified in additional data is supplied in the transmission instruction indicates location address is provided and now being used to access data in the server, see Suzuki, col. 6, lines 23-30), this concept can be implemented for transmitting address information of the location at which the second set of data is stored from said third node to said second node as it is done with the first set of data).

e) As to claim 15, the combination of Fronberg, Suzuki and Marvit discloses a method as claimed in claim 14, wherein the address information at which the second

set of data is stored is a URL. Marvit teaches the address information of the location at which the encrypted first set of data is stored is a URL (i.e. the recipient is provided with a message's URL that specifies the location of the message, see Marvit: col. 19, lines 55-59, this concept can be implemented to provide the address information at which the second set of data is stored is a URL as it is done with the first set of data).

f) As to claim 20, the combination of Fronberg and Suzuki discloses a method as claimed in claim 19, further comprising the steps of decrypting the encrypted first set of data (i.e. encrypting/decrypting process using the same key, see Fronberg: paragraphs 0046-0048), however it is silent on the capability of downloading the second set of data from the third node to the second node. Marvit is relied on for the teaching of downloading the second set of data from the third node to the second node (i.e. downloading key from key repository, see Marvit: col. 3, lines 52-55). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of downloading the second set of data from the third node to the second node in the system of Fronberg and Suzuki, as Marvit teaches, so as to be able to access to the protected data (see Marvit: col. 3, lines 48-50).

g) As to claim 25, the combination of Fronberg, Suzuki and Marvit discloses a method as claimed in claim 8, wherein the third node comprises a second network archive server (e.g. key repository, see Marvit: Fig. 2, element 106).

h) As to claim 39, this claim is directed to a system implementation of the method of claim 8, therefore it is rejected by a similar rationale applied against claim 8 above.

8. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Suzuki et al. (6,704,119) and further in view of Schneier ((Applied Cryptography).

The combination of Fronberg and Suzuki discloses a method as claimed in claim 6, however it is silent on the capability of decrypting the encrypted first set of data by performing an exclusive OR operation between the encrypted first set of data and the second set of data. Schneier is relied on for the teaching of decrypting the encrypted first set of data by performing an exclusive OR operation between the encrypted first set of data and the second set of data (i.e. the ciphertext is being XORed with a keyword to generate the plaintext, see Schneier: page 14). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data in the system of Fronberg and Suzuki, as Schneier teaches, so as to provide another way of decrypting data.

9. Claims 28 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Bloomberg (5,765,176).

a) As to claim 28, Fronberg discloses a method as claimed in claim 1, however he is silent on the capability of having the second set of data comprises one of a thumbnail image, an extract from an audio file or a picture of a multimedia message. Bloomberg is relied on for the teaching of the second set of data comprises one of a thumbnail image, an extract from an audio file or a picture of a multimedia message (i.e.

an icon image or thumbnail image represents larger document, see Bloomberg: col. 1,lines 28-51). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the second set of data comprises one of a thumbnail image, an extract from an audio file or a picture of a multimedia message in the system of Fronberg, as Bloomberg teaches, so as to perform document image management tasks related to the text image (see Bloomberg: col. 1, lines 25-27).

b) As to claim 50, this claim is directed to a system implementation of the method of claim 28, therefore it is rejected by a similar rationale applied against claim 28 above.

10. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Suzuki et al. (6,704,119) and further in view of Wang et al (6,173,406).

The combination of Fronberg and Suzuki discloses a method as claimed in claim 7, however it is silent on the capability of having the address information of a location at which the encrypted first set of data is stored, and the second set of data are sent to a third party. Wang is relied on for the teaching of having the address information of a location at which the encrypted first set of data is stored, and the second set of data (e.g. password) are sent to a third party (e.g. video server) (i.e. user provides specified URL, where URL links to a selected multimedia content, and password to the video server, see Wang: col. 5, lines 20-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the address

information of a location at which the encrypted first set of data is stored, and the second set of data are sent to a third party in the system of Fronberg and Suzuki, as Wang teaches so as to control content presentation and reproduction by unauthorized and unauthenticated users of media content distributed over networks (see Wang: col. 1, lines 35-38).

11. Claim 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Suzuki et al. (6,704,119) and further in view of Sull et al. (2002/0069218).

a) As to claim 32, the combination of Fronberg and Suzuki discloses a method as claimed in claim 11, however it is silent on the capability of having the address information of the location at which the encrypted first set of data is stored, is stored in the second set of data as a watermark. Sull is relied on for the teaching of having the address information of the location at which the encrypted first set of data is stored, is stored in the second set of data as a watermark (i.e. URL can be encoded into a thumbnail image and the image encoded with the texts can be used in watermarking technology, see Sull: paragraph 0265). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the address information of the location at which the encrypted first set of data is stored, is stored in the second set of data as a watermark in the system of Fronberg and Suzuki, as Sull teaches so as to facilitate storing, searching and retrieving the multimedia information (see Sull: paragraph 0002).

b) As to claim 33, the combination of Fronberg and Suzuki discloses a method as claimed in claim 11, however it is silent on the capability of having the address information of the location at which the encrypted first set of data is stored is derivable from the second set of data. Sull is relied on for the teaching of having the address information of the location at which the encrypted first set of data is stored, is derivable from the second set of data (i.e. URL of a video file can be encoded into a thumbnail image, therefore URL can be derivable from the thumbnail image, see Sull: paragraph 0265)). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the address information of the location at which the encrypted first set of data is stored is derivable from the second set of data in the system of Fronberg and Suzuki, as Sull teaches, so as to retrieve multimedia data using its location identification data encoded in thumbnail image.

12. Claims 41-42, 44-45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Schneier (Applied Cryptography) and in view of Suzuki (.

a) As to claim 41, the combination of Fronberg and Schneier discloses a system as claimed in claim 38, however it is silent on the capability of having the second node further comprises transmitting means configured to transmit the encrypted first set of data to the first node. Suzuki is relied on for the teaching of having the second node (e.g. MFP) further comprises transmitting means configured to transmit the encrypted first set of data to the first node (e.g. server) (see Suzuki: col. 12, lines

36-39). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the second node further comprises transmitting means configured to transmit the encrypted first set of data to the first node in the system of Fronberg and Schneier, as Suzuki teaches, so as to store and archive file data (see Suzuki: col. 1, lines 15-22).

b) As to claim 42, the combination of Fronberg and Schneier discloses a system as claimed in claim 38, however it is silent on the capability of having the second node further comprises a capturing means to capture the first set of data. Suzuki is relied on for the teaching of having the second node (e.g. MFP) further comprises a capturing means to capture the first set of data (i.e. MFP 11 can be used as a copy machine, a facsimile machine, a printer and a scanner, any of those devices can capture the first set of data, see Suzuki: col. 5, lines 27-28). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the second node further comprises a capturing means to capture the first set of data in the system of Fronberg and Schneier, as Suzuki teaches, so as to collect and process captured data (see Suzuki: col. 1, lines 15-22).

c) As to claim 44, the combination of Fronberg, Schneier and Suzuki discloses a system as claimed in claim 42, wherein the decrypting means is configured to decrypt the encrypted first set of data by performing an exclusive OR operation between the encrypted first set of data and the second set of data (i.e. the ciphertext is being XORed with a keyword to generate the plaintext, see Schneier: page 14).

d) As to claim 45, the combination of Fronberg and Schneier discloses a system as claimed in claim 36, however it is silent on having the first node comprises a first network archive server. Suzuki is relied on for the teaching of having the first node comprises a first network archive server (e.g. server 12, see Suzuki: col. 6, lines 31-40, lines 48-57). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the first node comprises a first network archive server in the system of Fronberg and Schneier, as Suzuki teaches, so as to store and archive file data (see Suzuki: col. 1, lines 15-22).

e) As to claim 47, the combination of Fronberg, Schneier and Suzuki discloses a system as claimed in claim 45, wherein the user equipment comprises one of a mobile station, a digital camera, a personal digital assistant or a personal computer (i.e. computer, see Fronberg: Fig. 1, element 112).

13. Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Schneier (Applied Cryptography) and further in view of Marvit (6,625,734).

The combination of Fronberg and Schneier discloses a system as claimed in claim 38, however it is silent on the capability of having the third node comprises a second network server archive. Marvit is relied on for the teaching of having the third node comprises a second network server archive (e.g. key repository, see Marvit: Fig. 2, element 106). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the third node comprises a second network

server archive in the system of Fronberg and Schneier, as Marvit teaches so as to store and archive processed data.

14. Claims 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fronberg (2004/0139317) in view of Marvit (6,625,734).

a) As to claim 52, Fronberg discloses a system as claimed in claim 34, however he is silent on the capability of having means are provided to delete the encrypted first set of data from the first node after the encrypted first set of data has been downloaded. Marvit is relied on for the teaching of having means are provided to delete the encrypted first set of data from the first node after the encrypted first set of data has been downloaded (i.e. deletion message from specified location after message has been retrieved from the specified location, see Marvit: col. 18, lines 42-45). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having means are provided to delete the encrypted first set of data from the first node after the encrypted first set of data has been downloaded in the system of Fronberg, as Marvit teaches, so as to control storing and archiving processed data.

b) As to claim 53, Fronberg discloses a system as claimed in claim 34, however he is silent on the capability of having a node for storing the encrypted first set of data. Marvit is relied on for the teaching of having a node for storing the encrypted first set of data (i.e. message repository for storing the encrypted message, see Marvit: col. 18, lines 46-60). It would have been obvious to one of ordinary skill in the art at the

time of the invention to employ the use of having a node for storing the encrypted first set of data in the system of Fronberg, as Marvit teaches so as to provide a means for storing and archiving processed data.

c) As to claim 54, the combination of Fronberg and Marvit discloses a system as claimed in claim 52, wherein said node is a network archive server (e.g. message repository, see Marvit: Fig. 9, element 906).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
1/3/07